ON IDEAL LATTICES AND GRÖBNER BASES

MARIA FRANCIS AND AMBEDKAR DUKKIPATI

Abstract. In this paper, we draw a connection between ideal lattices and Gröbner bases in the multivariate polynomial rings over integers. We study extension of ideal lattices in $\mathbb{Z}[x]/\langle f\rangle$ (Lyubashevsky & Micciancio, 2006) to ideal lattices in $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$, the multivariate case, where f is a polynomial in $\mathbb{Z}[X]$ and $\mathfrak{a}$ is an ideal in $\mathbb{Z}[x_1,\ldots,x_n]$. Ideal lattices in univariate case are interpreted as generalizations of cyclic lattices. We introduce a notion of multivariate cyclic lattices and we show that multivariate ideal lattices are indeed a generalization of them. We show that the fact that existence of ideal lattice in univariate case if and only if f is monic translates to short reduced Gröbner basis (Francis & Dukkipati, 2014) of $\mathfrak{a}$ is monic in multivariate case. We, thereby, give a necessary and sufficient condition for residue class polynomial rings over $\mathbb{Z}$ to have ideal lattices. We also characterize ideals in $\mathbb{Z}[x_1,\ldots,x_n]$ that give rise to full rank lattices.

1. Introduction

After Ajtai (1996) built functions that on an average generated hard instances of standard lattice problems, research progressed in the direction of building cryptographic primitives based on them. The fundamental challenge to this direction of research was describing lattices as $n\times n$ integer matrices since that meant the size of the key and the computation time of the cryptographic functions will be atleast quadratic in n. Micciancio (2002) used a class of lattices called 'cyclic lattices' to build certain efficient one-way functions called generalized compact knapsack functions.

Lattices that are closed under cyclic shifts are called cyclic lattices and these are integer lattices that are also ideals in $\mathbb{Z}[x]/\langle x^n-1\rangle$. The advantage of cyclic lattices is that they have a compact representation and therefore the time taken for these functions is almost linear in n (Micciancio, 2002). But one way functions are of theoretical interest and can not be used to build useful cryptographic primitives (Lyubashevsky & Micciancio, 2006). In (Lyubashevsky & Micciancio, 2006) a new class of lattices called 'ideal lattices' were introduced and efficient collision resistant hash functions were designed using them.

Ideal lattices are ideals in a quotient ring $\mathbb{Z}[x]/\langle f\rangle$, for any monic polynomial $f\in\mathbb{Z}[x]$, that are also lattices. This is due to the fact that $\mathbb{Z}[x]/\langle f\rangle$ is isomorphic to $\mathbb{Z}^N$ if and only if f is monic. In fact, in cryptographic applications the choice of f is further restricted to

irreducible polynomials. Over the years, ideal lattices have been used to build several cryptographic primitives that include digital signatures (Lyubashevsky & Micciancio, 2008), hash functions (Lyubashevsky & Micciancio, 2006) and identification schemes (Lyubashevsky, 2008).

On the other hand, any extension of solutions of problems from one variable case to multivariate case, in particular, in algebra, have led to important theories, an example being the theory of Gröbner bases introduced by Buchberger (1965), that has become a standard tool in algorithmic aspects of commutative algebra and algebraic geometry. The reason is computing Gröbner bases of ideals in multivariate case is enough to extend solutions of various problems from univariate to multivariate case. In this paper, we study ideal lattices from an algebraic point of view, and show how Gröbner bases play a role in the study of extending ideal lattices from univariate case to multivariate case. In fact, we give a necessary and sufficient condition for residue class polynomial rings over $\mathbb{Z}$ to have ideal lattices, in terms of 'short reduced Gröbner bases' that was introduced in (Francis & Dukkipati, 2014).

Contributions. In this paper, we study ideal lattices in the multivariate case. That is, given an ideal $\mathfrak{a}$ in $\mathbb{Z}[x_1, \ldots, x_n]$ we study cases for which ideals in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ are also lattices. As in the univariate counterpart, we show that ideal lattices in the multivariate case are also a generalization of introduced objects called multivariate cyclic lattices. We show that ideal lattices exists only when the residue class polynomial ring over $\mathbb{Z}$ is a free $\mathbb{Z}$-module, for which we give a characterization based on short reduced Gröbner bases. Short reduced Gröbner bases were introduced in (Francis & Dukkipati, 2014) to characterize free A-modules $A[x_1, \ldots, x_n]/\mathfrak{a}$, where A is a Noetherian ring and $\mathfrak{a}$ is an ideal in $A[x_1, \ldots, x_n]$. For the construction of many cryptographic primitives full rank lattices are essential and we derive the condition for an ideal lattice in the multivariate case to be a full rank lattice. We also give an example of a class of binomial ideals in $\mathbb{Z}[x_1, \ldots, x_n]$, where the residue class polynomial ring gives rise to full rank integer lattices.

Outline of the paper. The rest of the paper is organized as follows. In Section 2, we look at preliminaries relating to lattices and ideal lattices. In Section 3, we study cyclic lattices in the multivariate case. In Section 4, we prove that only free and finitely generated $\mathbb{Z}$-modules have ideal lattices. Finally, we give a characterization for ideal lattices to be full rank in Section 5.

2. Background & Preliminaries

Let $\Bbbk$ be a field, A a Noetherian commutative ring, $\mathbb{Z}$ the ring of integers and $\mathbb{N}$ the set of positive integers including zero. Let $\mathbb{R}^m$ be the m-dimensional Euclidean space.

A polynomial ring in an indeterminate x is denoted by $A[x]$. In the multivarite case polynomial ring in indeterminates $x_1, \ldots, x_n$ over A is denoted by $A[x_1, \ldots, x_n]$. A monomial $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ in $x_1, \ldots, x_n$ is denoted by x^α, where $\alpha \in \mathbb{Z}^n_{\geq 0}$. If an ideal $\mathfrak{a}$ in $A[x_1, \ldots, x_n]$ is generated by $f_1, \ldots, f_s \in A[x_1, \ldots, x_n]$ then we write $\mathfrak{a} = \langle f_1, \ldots, f_s \rangle$.

Now we recall some preliminaries on lattices. For a good exposition one can refer to (Micciancio & Goldwasser, 2002).

Definition 2.1. *A lattice in $\mathbb{R}^m$ is the set*

$$\mathcal{L}(b_1, \ldots, b_n) = \{\sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z}\}$$

of all integral combinations of n linearly independent vectors $b_1, \ldots, b_n$ in $\mathbb{R}^m (m \geq n)$.

The integers n and m are called the rank and dimension of the lattice, respectively. The sequence of vectors $b_1, \ldots, b_n$ is called a lattice basis. When $n = m$, we say that $\mathcal{L}$ is full rank or full dimensional. An example of n-dimensional lattice is the set $\mathbb{Z}^n$ of all vectors with integral coordinates. In sequel, whenever we mention lattices we mean integer lattices, lattices where the basis vectors have integer coordinates. Integer lattices are additives subgroups of $\mathbb{Z}^N$, $N \in \mathbb{N}$.

An ideal lattice[1] is an integer lattice $\mathcal{L} \subseteq \mathbb{Z}^N$ that is also an ideal in $\mathbb{Z}[x]/\langle f \rangle$ for some monic polynomial $f \in \mathbb{Z}[x]$. We now formally define ideal lattices in one variable.

Definition 2.2. *Given a monic polynomial $f \in \mathbb{Z}[x]$, an ideal lattice is an integer lattice $\mathcal{L} \subseteq \mathbb{Z}^N$ such that it is isomorphic, as a $\mathbb{Z}$-module, to an ideal $\mathfrak{A}$ in $\mathbb{Z}[x]/\langle f \rangle$.*

The following $\mathbb{Z}$-module homomorphism between $\mathbb{Z}[x]/\langle f \rangle$ and $\mathbb{Z}^N$, where f is a monic polynomial of degree N, further elucidates the definition of ideal lattices.

$$\begin{aligned} \psi : \mathbb{Z}[x]/\langle f \rangle &\longrightarrow \mathbb{Z}^N \\ \sum_{i=0}^{N-1} a_i x^i + \langle f \rangle &\longmapsto (a_0, \cdots, a_{N-1}). \end{aligned}$$

[1]We feel that the definition given in (Lyubashevsky & Micciancio, 2006) is not mathematically accurate which reads as the following. *An ideal lattice is an integer lattice $\mathcal{L} \subseteq \mathbb{Z}^N$ such that it is also an ideal in $\mathbb{Z}[x]/\langle f \rangle$, i.e. $\mathcal{L} = \{g \mod f \mid g \in \mathfrak{A}\}$ for some monic polynomial $f \in \mathbb{Z}[x]$ of degree N and ideal $\mathfrak{A} \subseteq \mathbb{Z}[x]/\langle f \rangle$.*

Clearly, ψ is an isomorphism that implies all $\mathbb{Z}$-modules (including ideals) in $\mathbb{Z}[x]/\langle f\rangle$ are isomorphic to sublattices (subgroups) of $\mathbb{Z}^N$. Therefore, all ideals in $\mathbb{Z}[x]/\langle f\rangle$ are ideal lattices. The main aim of this paper is to extend the concept of ideal lattices to the multivariate case.

3. Multivariate Cyclic Lattices

Before we look into the multivariate case we recall the definition of cyclic lattices.

Definition 3.1. *A set $\mathcal{L}$ in $\mathbb{Z}^N$ is a cyclic lattice*

(i) for all $v, w \in \mathcal{L}$, $v + w$ is also in $\mathcal{L}$,
(ii) for all $v \in \mathcal{L}$, $-v$ is also in $\mathcal{L}$, and
(iii) for all $v \in \mathcal{L}$, a cyclic shift of v is also in $\mathcal{L}$.

One can easily verify the following fact.

Lemma 3.2. *A set $\mathcal{L}$ in $\mathbb{Z}^N$ is a cyclic lattice if $\mathcal{L}$ is an ideal in $\mathbb{Z}[x]/\langle x^N - 1\rangle$.*

Now consider $\mathbb{Z}[x_1, \dots, x_n]/\langle {x_1}^{r_1} - 1, {x_2}^{r_2} - 1, \cdots, {x_n}^{r_n} - 1\rangle$, for some $r_1, \dots, r_n \in \mathbb{N}$. Let $\mathfrak{a} = \langle {x_1}^{r_1} - 1, \cdots, {x_n}^{r_n} - 1\rangle$ and $r_1 \times r_2 \times \cdots \times r_n = N$. We have $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ is a free $\mathbb{Z}$-module, isomorphic to $\mathbb{Z}^N$ with $\mathcal{B} = \{{x_1}^{\alpha_1} \dots {x_n}^{\alpha_n} + \mathfrak{a}, \alpha_k \in \{0, \dots, r_k - 1\}\}$ as a $\mathbb{Z}$-module basis. Given an element of the residue class polynomial ring,

$$\sum_{j=1}^{N} a_{(\alpha_{1j},\dots,\alpha_{nj})} {x_1}^{\alpha_{1j}} \dots {x_n}^{\alpha_{nj}} + \mathfrak{a},$$

where $\alpha_{kj} \in \{0, \dots, r_k - 1\}$ and $a_{(\alpha_{1j},\dots,\alpha_{nj})} \in \mathbb{Z}$, one can represent it using a tensor, $\mathcal{A} \in \mathbb{Z}^{r_1 \times \cdots \times r_n}$ such that

$$\mathcal{A}_{i_1,\dots,i_n} = a_{(i_1-1,\dots,i_n-1)},$$

where $A_{i_1,\dots,i_n}$ denotes $(i_1, \dots, i_n)$ element in the tensor $\mathcal{A}$.

Now consider $\mathbb{Z}^N$ and suppose $r_1, \dots, r_n \in \mathbb{N}$ such that $r_1 \times r_2 \times \cdots \times r_n = N$. Given a lattice $\mathcal{L} \subseteq \mathbb{Z}^N$ where $\mathbb{Z}^N = \mathbb{Z}^{r_1 \times \cdots \times r_n}$, it is easy to see that a one-to-one correspondence exists between a vector in $\mathcal{L}$ and a tensor in $\mathbb{Z}^{r_1 \times \cdots \times r_n}$.

Let $\mathcal{A}$ be a tensor in $\mathbb{Z}^{r_1 \times \cdots \times r_n}$. We define a $(n-1)^{\text{th}}$ order tensor for each $r_i \in \{1, \dots, n\}$ and denote it as $A_i(j)$ where $A_i(j) \in \mathbb{Z}^{r_1 \times r_2 \times \cdots \times r_{i-1} \times r_{i+1} \times \cdots \times r_n}$. We have,

$$A_i(j)_{(k_1,\dots,k_{i-1},k_{i+1},\dots,k_n)} = \mathcal{A}_{(k_1,\dots,k_{i-1},j,k_{i+1},\dots,k_n)}, \ \ j \in \{0, \dots, r_i - 1\}.$$

We construct the following ordered set of $(n-1)^{\text{th}}$ order tensors for each $r_i \in \{1, \dots, n\}$,

$$\mathcal{A}_i = (A_i(0), A_i(1), \cdots, A_i(r_i - 1)).$$

Using this set, we introduce the notion of multivariate cyclic shifts.

Definition 3.3. *Let $\mathcal{L} \subseteq \mathbb{Z}^N = \mathbb{Z}^{r_1\times\cdots\times r_n}$ be a lattice and $\mathcal{A} \in \mathbb{Z}^{r_1\times\cdots\times r_n}$, a tensor in $\mathcal{L}$. The i^{th}-multivariate cyclic shift of $\mathcal{A}$, $\sigma_i(\mathcal{A})$ is a cyclic shift of elements in the ordered set, $\mathcal{A}_i$.*

Observe that multiplying an element in $\mathbb{Z}[x_1, \dots, x_n]/\langle {x_1}^{r_1} - 1, \cdots, {x_n}^{r_n} - 1\rangle$ with x_i results in a cyclic shift in the ordered set, $\mathcal{A}_i$. This is also equivalent to a cyclic permutation in the n^{th} order tensor along the i^{th} direction.

We now formerly define multivariate cyclic lattices.

Definition 3.4. *A set $\mathcal{L}$ in $\mathbb{Z}^N = \mathbb{Z}^{r_1\times\cdots\times r_n}$ is a multivariate cyclic lattice if*

(i) for all $v, w \in \mathcal{L}$, $v + w$ is also in $\mathcal{L}$,
(ii) for all $v \in \mathcal{L}$, $-v$ is also in $\mathcal{L}$, and
(iii) for all $v \in \mathcal{L}$, a i^{th}-multivariate cyclic shift of v is also in $\mathcal{L}$ for all $i \in \{1, \dots, n\}$.

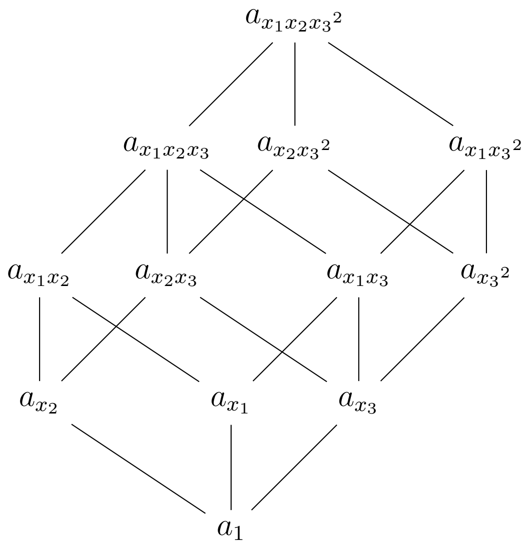
We illustrate this with the following example.

Example 3.5. *Consider the case when $n = 3$ and we have $r_1 = 2$, $r_2 = 2$ and $r_3 = 3$. The quotient ring associated to it is $\mathbb{Z}[x_1, x_2, x_3]/\langle {x_1}^2 - 1, {x_2}^2 - 1, {x_3}^3 - 1\rangle$. It is isomorphic to the space of 3^{rd} order tensors, $\mathbb{Z}^{2\times2\times3} (\cong \mathbb{Z}^{12})$. The following set of monomials form the set of coset representatives for a $\mathbb{Z}$-module basis,*

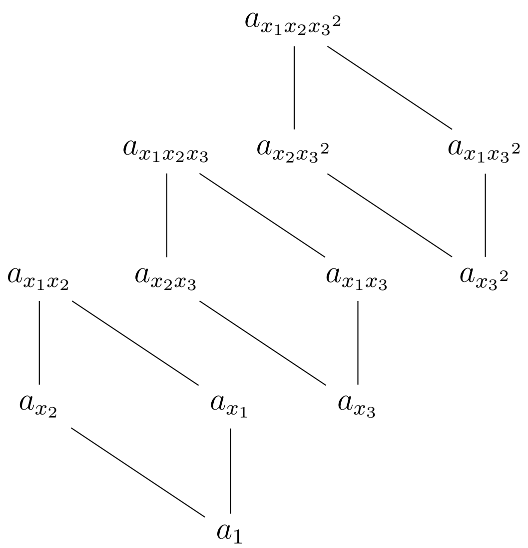
$$\{1, x_1, x_2, x_3, {x_3}^2, x_1x_2, x_1x_3, x_1{x_3}^2, x_2x_3, x_2{x_3}^2, x_1x_2x_3, x_1x_2{x_3}^2\}.$$

Any element in the residue class ring can be represented as a 3^{rd} order tensor, $\mathcal{A} \in \mathbb{Z}^{2\times2\times3}$. Let a_{x^α} be the coefficient of the basis element, x^α. We can represent $\mathcal{A}$ as follows,

$\mathcal{A} =$



The following tensors represent $A_3(0)$, $A_3(1)$ and $A_3(2)$ respectively.



.

$A_3(0)$, $A_3(1)$ and $A_3(2)$ represent 2^{nd} order tensors corresponding to $x_3 = 0$, $x_3 = 1$ and $x_3 = 2$ respectively. Similarly, $A_2(0)$ and $A_2(1)$ represent 2^{nd} order tensors corresponding to $x_2 = 0$ and $x_2 = 1$ and $A_1(0)$ and $A_1(1)$ represent 2^{nd} order tensors corresponding to $x_1 = 0$ and $x_1 = 1$. Multiplying with x_3 here results in a cyclic rotation of $A_3(0)$, $A_3(1)$ and $A_3(2)$.

Multiplying with a monomial ${x_1}^{\alpha_1} \cdots {x_n}^{\alpha_n}$ in the general case results in a composition of α_i shifts in $\mathcal{A}_i$ for each $i \in \{1, \ldots, n\}$. The commutativity of multiplication is taken care of as the shifts act on an independent set of subtensors and this makes the order of the composition of cyclic shifts irrelevant, i.e. the order in which we perform the cyclic shifts between $\mathcal{A}_i$ and $\mathcal{A}_j$ does not matter for $i, j \in \{1, \ldots, n\}$.

Finally we state the following.

Proposition 3.6. *Every ideal in*

$$\mathbb{Z}[x_1, \ldots, x_n]/\langle {x_1}^{r_1} - 1, {x_2}^{r_2} - 1, \cdots, {x_n}^{r_n} - 1\rangle$$

is a multivariate cyclic lattice.

4. Multivariate Ideal Lattices and Short Reduced Gröbner Basis

Ideal lattices in the multivariate case can be defined in a similar way. A multivariate ideal lattice is an integer lattice $\mathcal{L} \subseteq \mathbb{Z}^N$ that is also an ideal in $\mathbb{Z}[x]/\mathfrak{a}$ for some ideal $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$. The definition is as follows.

Definition 4.1. *Given an ideal $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$, a multivariate ideal lattice is an integer lattice $\mathcal{L} \subseteq \mathbb{Z}^N$ such that it is isomorphic, as a $\mathbb{Z}$-module, to an ideal $\mathfrak{A}$ in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$.*

In sequel, we mention multivariate ideal lattices as just ideal lattices and it should be clear from the context.

The $\mathbb{Z}$-module structure of $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ is crucial in locating ideal lattices in $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$. In general, for a Noetherian ring A, one can use Gröbner basis methods to determine the A-module structure of $A[x_1,\ldots,x_n]/\mathfrak{a}$, where $\mathfrak{a}$ is an ideal in $A[x_1,\ldots,x_n]$ (Francis & Dukkipati, 2014). We describe this briefly below.

Consider an ideal $\mathfrak{a} \subseteq A[x_1,\ldots,x_n]$. Let $G = \{g_i : i = 1,\ldots,t\}$ be a Gröbner basis for $\mathfrak{a}$. Let $J_{x^\alpha} = \{i : \mathrm{lm}(g_i) \mid x^\alpha, g_i \in G\}$ and $I_{J_{x^\alpha}} = \langle\{\mathrm{lc}(g_i) : i \in J_{x^\alpha}\}\rangle$. Here $\mathrm{lm}(g_i)$ denotes leading monomial of the polynomial g_i and $\mathrm{lm}(g_i)$ denotes leading coefficient. We refer to $I_{J_{x^\alpha}}$ as the leading coefficient ideal w.r.t. G. Here we assume that the coefficient ring A has effective coset representatives (Adams & Loustaunau, 1994, pp 226). Let $C_{J_{x^\alpha}}$ represent a set of coset representatives of the equivalence classes in $A/I_{J_{x^\alpha}}$. On reducing $f \in A[x_1,\ldots,x_n]$ with G we get $f = \sum\limits_{i=1}^{m} a_i x^{\alpha_i} \mathrm{mod}\langle G\rangle$, where $a_i \in A, i = 1,\ldots,m$. If $A[x_1,\ldots,x_n]/\langle G\rangle$ is a finitely generated A-module of size m, then corresponding to coset representatives, $C_{J_{x^{\alpha_1}}},\ldots,C_{J_{x^{\alpha_m}}}$, there exists an A-module isomorphism (Francis & Dukkipati, 2014)

$$\begin{aligned} \phi : A[x_1,\ldots,x_n]/\langle G\rangle &\longrightarrow A/I_{J_{x^{\alpha_1}}} \times \cdots \times A/I_{J_{x^{\alpha_m}}} \\ \sum_{i=1}^{m} a_i x^{\alpha_i} + \langle G\rangle &\longmapsto (c_1 + I_{J_{x^{\alpha_1}}}, \cdots, c_m + I_{J_{x^{\alpha_m}}}), \end{aligned} \tag{1}$$

where $c_i = a_i \bmod I_{J_{x^{\alpha_i}}}$ and $c_i \in C_{J_{x^{\alpha_i}}}$. When $I_{J_{x^{\alpha_i}}} = \{0\}$, for all $i \in \{1,\ldots,m\}$ we have $C_{J_{x^{\alpha_i}}} = A$, for all $i \in \{1,\ldots,m\}$. This implies $A[x_1,\ldots,x_n]/\mathfrak{a} \cong A^m$. In this case, in particular, when $A = \mathbb{Z}$, $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ is a free $\mathbb{Z}$-module. One can conclude that corresponding to every ideal in $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ there exists a subgroup in $\mathbb{Z}^n$, hence it is an ideal lattice.

Proposition 4.2. *Every ideal in a free and finitely generated $\mathbb{Z}$-module, $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ is an ideal lattice.*

Our next step is to determine if residue class polynomial rings with torsion submodules contain ideal lattices. Using the structure theorem for finitely generated modules over a PID (Adkins & Weintraub, 1992, Chapter 3, Theorem 7.1), determination of the existence of ideal lattices in a finitely generated $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ with torsion is relatively straightforward.

Proposition 4.3. *If a finitely generated $\mathbb{Z}$-module, $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ is not free then no ideal in $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ is an integer lattice.*

Proof. We have from the structure theorem over a PID,

$$\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a} \cong \mathbb{Z}^l \oplus \mathbb{Z}/\langle w_1\rangle \oplus \cdots \oplus \mathbb{Z}/\langle w_k\rangle.$$

If there is no free part then clearly the residue class ring does not have an ideal lattice. Let G be the Gröbner basis of the ideal, $\mathfrak{a}$. Assume there exists an ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ such that it is an integer lattice. Let $x^{\alpha_r} + \mathfrak{a} \in \mathfrak{A}$ be an element such that the leading coefficient ideal of x^{α_r} in $\mathbb{Z}$, $I_{J_{x^{\alpha_r}}}$ is equal to $\{0\}$. This implies that the set of coset representatives, $C_{J_{x^{\alpha_r}}} = \mathbb{Z}$ and therefore the monomial corresponds to the free part. Consider the ideal generated by $x^{\alpha_r} + \mathfrak{a}$. Since the $\mathbb{Z}$-module is not free we have $I_{J_{x^{\alpha_j}}} \neq \{0\}$ for some monomial x^{α_j} in Equation (1). Let $c \in C_{J_{x^{\alpha_j}}}$. We have, $cx^{\alpha_j}x^{\alpha_r} + \mathfrak{a} \in \langle x^{\alpha_r} + \mathfrak{a}\rangle$. This implies the ideal generated by a free element contains torsion elements. Thus the $\mathbb{Z}$-module $\mathfrak{A}$ has torsion elements and is not isomorphic to an integer lattice which is a contradiction. □

Thus we have the following result.

Corollary 4.4. *Every ideal, $\mathfrak{a}$ in $\mathbb{Z}[x_1,\ldots,x_n]$ is an ideal lattice if and only if $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ is a free and finitely generated $\mathbb{Z}$-module.*

To test whether a $\mathbb{Z}$-module $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ is free, algorithmically, one needs the notion of 'short reduced Gröbner bases' introduced in (Francis & Dukkipati, 2014). We describe this here for any polynomial ring over a Noetherian ring, A.

Definition 4.5. *Let $\mathfrak{a} \subseteq A[x_1,\ldots,x_n]$ be an ideal. A reduced Gröbner basis G of $\mathfrak{a}$ is called a short reduced Gröbner basis if for each $x^\alpha \in \mathrm{lm}(G)$, the length of the generating set for its leading coefficient ideal is minimal.*

The reduced Gröbner basis in the above definition is as described in (Pauer, 2007). Short reduced Gröbner basis is a reduced Gröbner basis with an additional condition that the length of the generating set of the leading coefficient ideals in the basis is minimal. When $A = \mathbb{Z}$ in the above proposition, short reduced Gröbner basis is the reduced Gröbner basis of $\mathfrak{a}$ where the generator of the leading coefficient ideal is taken as the *gcd* of all generators.

We now give the characterization.

Proposition 4.6. *Let $\mathfrak{a} \subseteq A[x_1,\ldots,x_n]$ be a non-zero ideal such that $A[x_1,\ldots,x_n]/\mathfrak{a}$ is finitely generated. Let G be a short reduced Gröbner basis for $\mathfrak{a}$ w.r.t. some monomial ordering. Then,*

$$A[x_1,\ldots,x_n]/\mathfrak{a} \cong A^N, \quad \textit{for some } N \in \mathbb{N}$$

if and only if G is monic.

We can summarize the results in this section by the theorem below.

Theorem 4.7. *The $\mathbb{Z}$-module, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ has ideal lattices if and only if the short reduced Gröbner basis of $\mathfrak{a}$ is monic.*

We illustrate this by an example.

Example 4.8. *Let $\mathfrak{a} = \langle 3x^2, 5x^2, y \rangle$ be an ideal in $\mathbb{Z}[x, y]$. The short reduced Gröbner basis for the ideal is $G = \{x^2, y\}$. Since G is monic $\mathbb{Z}[x, y]/\mathfrak{a}$ is free and isomorphic to $\mathbb{Z}^2$. All ideals in it are ideal lattices. For example the ideal generated by $6x + \langle x^2, y \rangle$ is isomorphic to the lattice, $\mathcal{L}([(0, 6)])$. Note that here $\mathcal{L}([(0, 6)])$ denotes the subgroup generated by $(0, 6)$ in $\mathbb{Z}^2$.*

5. Full Rank Lattices in Free, Finitely Generated $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$

We recall that in the definition of ideal lattices in $\mathbb{Z}[x]$ the choice of the polynomial f in $\mathbb{Z}[x]/\langle f \rangle$ is restricted to monic polynomials. But in the construction of many cryptographic primitives like collision resistant hash functions an additional condition is imposed on f that f is an irreducible polynomial. This condition ensures that the lattice is full rank that is fundamental in many cryptographic constructions (Lyubashevsky & Micciancio, 2006). In multivariate case, we derive a necessary and sufficient condition for ideal lattices to be full rank.

Proposition 5.1. *Let $\{g_1, \ldots, g_t\}$ be a monic short reduced Gröbner basis of an ideal $\mathfrak{a}$ in $\mathbb{Z}[x_1, \ldots, x_n]$ such that $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a} \cong \mathbb{Z}^N$ for some $N \in \mathbb{N}$. All ideals in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ are full rank lattices if and only if $\mathfrak{a}$ is a prime ideal.*

Proof. Let $\mathfrak{a} = \langle g_1, \cdots, g_t \rangle$ be a prime ideal. Consider an ideal $\mathfrak{A} = \langle f_1 + \mathfrak{a}, \cdots, f_s + \mathfrak{a} \rangle$ in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. Since $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a} \cong \mathbb{Z}^N$ we have a finite basis, $\mathcal{B} = \{b_1 + \mathfrak{a}, \ldots, b_N + \mathfrak{a}\}$. We have to prove that there are N linearly independent vectors in $\mathfrak{A}$. Consider $f_1 b_1, \ldots, f_1 b_N$. Let $c_1 f_1 b_1 + \cdots + c_N f_1 b_N \in \langle g_1, \cdots, g_t \rangle$. This implies $f_1(c_1 b_1 + \cdots + c_N b_N) \in \langle g_1, \cdots, g_t \rangle$. Since $\langle g_1, \cdots, g_t \rangle$ is a prime ideal, either $f_1 \in \langle g_1, \cdots, g_t \rangle$ or $(c_1 b_1 + \cdots + c_N b_N) \in \langle g_1, \cdots, g_t \rangle$. But both cases cannot happen. Therefore $c_i = 0$ for all $i \in \{1, \ldots, N\}$. This implies that $f_1 b_1 + \mathfrak{a}, \ldots, f_1 b_N + \mathfrak{a}$ are linearly independent and the ideal lattice is full rank.

Conversely, assume that $\mathfrak{a}$ is not a prime ideal. Then there exists $l, h \in \mathbb{Z}[x_1, \ldots, x_n]$ such that $lh \in \langle g_1, \cdots, g_t \rangle$ but $l \notin \langle g_1, \cdots, g_t \rangle$ and $h \notin \langle g_1, \cdots, g_t \rangle$. This implies, $l = \sum_{i=1}^{N} c_i b_i$ and $h = \sum_{i=1}^{N} d_i b_i$ where $b_i + \mathfrak{a} \in \mathcal{B}$, the basis for $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ and $c_i, d_i \in \mathbb{Z}$. Consider the ideal lattice $\langle l + \mathfrak{a} \rangle$. We have $lh \in \langle g_1, \cdots, g_t \rangle$. This implies $l \sum_{i=1}^{N} d_i b_i \in \langle g_1, \cdots, g_t \rangle$. But $l \notin \langle g_1, \cdots, g_t \rangle$ and $\sum_{i=1}^{N} d_i b_i \notin \langle g_1, \cdots, g_t \rangle$. The set $\{lb_1 + \mathfrak{a}, \ldots, lb_N + \mathfrak{a}\}$ contains linearly dependent

vectors and the rank of the ideal lattice $\langle l + \mathfrak{a} \rangle$ is $\lneq N$. Therefore, if the ideal $\mathfrak{a}$ is not a prime ideal then there are lattices in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ that are not full rank. $\square$

Determining if an ideal is prime or not is key to ideal lattices finding a practical application. An algorithm for primality testing in polynomial rings over any commutative, Noetherian ring, A can be found in (Gianni *et al.*, 1988).

We now give an example of a class of binomial ideals that are prime and give rise to free residue class polynomial rings. A lattice ideal, $\mathfrak{a}_{\mathcal{L}}$ in $\mathbb{k}[x_1, \ldots, x_n]$ is defined as the binomial ideal generated by $\{x^{v^+} - x^{v^-}\}$ where v^+ and v^- are non-negative with disjoint support and $v^+ - v^- \in \mathcal{L}$, where $\mathcal{L}$ is a lattice (Katsabekis *et al.*, 2010). Lattice ideals in polynomial rings over $\mathbb{Z}$ can be defined in the same way. In this case, the binomial ideal is generated over the polynomial ring, $\mathbb{Z}[x_1, \ldots, x_n]$. The generators of the ideal are binomials with the terms having opposite sign and the coefficients of both the terms equal to absolute value 1. One can show that the short reduced Gröbner basis of the lattice ideal is monic (Francis & Dukkipati, 2014). In this case, by Proposition 4.6, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}_{\mathcal{L}}$ is free.

Theorem 5.2. *Every ideal in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}_{\mathcal{L}}$, where $\mathfrak{a}_{\mathcal{L}}$ is a lattice ideal, is an ideal lattice.*

The saturation of an integer lattice, $\mathcal{L} \subseteq \mathbb{Z}^m$ is the lattice,

$$Sat(\mathcal{L}) = \{\alpha \in \mathbb{Z}^m \mid d\alpha \in \mathcal{L} \text{ for some } d \in \mathbb{Z}, d \neq 0\}.$$

We say that an integer lattice $\mathcal{L}$ is saturated if $\mathcal{L} = Sat(\mathcal{L})$. It can be easily shown that the lattice ideal $\mathfrak{a}_{\mathcal{L}}$ is prime if and only if $\mathcal{L}$ is saturated. Note that prime lattice ideals are also called toric ideals. For more details on toric ideals in $\mathbb{k}[x_1, \ldots, x_n]$ one can refer to (Bigatti *et al.*, 1999). The definitions related to toric ideals can be extended to polynomial rings over $\mathbb{Z}$ in a similar way. Thus, toric ideals in $\mathbb{Z}[x_1, \ldots, x_n]$ give rise to full rank integer lattices.

Summary

In this paper, we studied ideal lattices in the multivariate case and showed the use of Gröbner bases in locating them. We also introduced multivariate cyclic lattices to draw parallels between the univariate and multivariate cases. In particular, we showed that ideal lattices in multivariate case are a generalization of multivariate cyclic lattices. Using short reduced Gröbner bases, we have given an algorithmic method to identify ideals in $\mathbb{Z}[x_1, \ldots, x_n]$ that give rise to ideal lattices in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. Generating lattices of full rank is important

for cryptographic applications and we provide a necessary and sufficient condition for ideals in $\mathbb{Z}[x_1, \ldots, x_n]$ for the same.

Acknowledgments

The authors would like to thank Debarghya Ghoshdastidar for useful discussions on tensor representations of cyclic lattices in the multivariate case.

References

Adams, W. & Loustaunau, P. (1994). *An Introduction to Gröbner Bases.* American Mathematical Society.

Adkins, W. A. & Weintraub, S. H. (1992). *Algebra: An Approach Via Module Theory.* Springer.

Ajtai, M. (1996). Generating Hard instances of Lattice Problems (Extended Abstract). In: *Proceedings of the 1996 ACM Symposium on the Theory of Computing, STOC* (Miller, G. L., ed.). ACM.

Bigatti, A., La Scala, R. & Robbiano, L. (1999). Computing Toric Ideals. *Journal of Symbolic Computation* **27**(4), 351 – 365.

Buchberger, B. (1965). *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal (in German).* Ph.D. thesis, University of Innsbruck, Austria. (reprinted in Buchberger (2006)).

Buchberger, B. (2006). Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of Symbolic Computation* **41**, 475–511.

Francis, M. & Dukkipati, A. (2014). On reduced Gröbner basis and macaulay-buchberger basis theorem over noetherian rings. *Journal of Symbolic Computation* **DOI:10.1016/j.jsc.2014.01.001**.

Gianni, P., Trager, B. & Zacharias, G. (1988). Grbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation* **6**(23), 149 – 167.

Katsabekis, A., Morales, M. & Thoma, A. (2010). Binomial generation of the radical of a lattice ideal. *Journal of Algebra* **324**(6), 1334 – 1346.

Lyubashevsky, V. (2008). Lattice Based Identification Schemes Secure Under Active Attacks. In: *Proceedings of the 11th International Workshop on Practice and Theory in Public Key Cryptography, 2008* (Cramer, R., ed.), vol. 4939 of *Lecture Notes in Computer Science*. Springer.

Lyubashevsky, V. & Micciancio, D. (2006). Generalized Compact Knapsacks Are Collision Resistant. In: *ICALP (2)* (Bugliesi, M., Preneel, B., Sassone, V. & Wegener, I., eds.), vol. 4052 of *Lecture Notes in Computer Science*. Springer.

Lyubashevsky, V. & Micciancio, D. (2008). Asymptotically Efficient Lattice-Based Digital Signatures. In: *Theory of Cryptography Conference, 2008* (R., C., ed.), vol. 4948 of *Lecture Notes in Computer Science*. Springer.

Micciancio, D. (2002). Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions from Worst-Case Complexity Assumptions. In: *Symposium on Foundations of Computer Science (FOCS 2002) Proceedings*. IEEE Computer Society.

Micciancio, D. & Goldwasser, S. (2002). *Complexity of Lattice Problems: a cryptographic perspective*, vol. 671 of *The Kluwer International Series in Engineering and Computer Science*. Boston, Massachusetts: Kluwer Academic Publishers.

Pauer, F. (2007). Gröbner Bases with Coefficients in Rings. *Journal of Symbolic Computation* **42**(11-12).

E-mail address: mariaf@csa.iisc.ernet.in, ad@csa.iisc.ernet.in

Department of Computer Science & Automation, Indian Institute of Science, Bangalore - 560012